



2183  
#6

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:

BROWN, et al.

Serial No.: 09/895,801

Filed: June 29, 2001

Confirmation No.: 5589

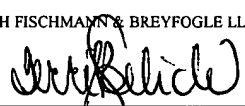
Atty. File No.: 41992-00427

For: "AUTOMATIC INFORMATION  
SANITIZER"

) Group Art Unit: 2183

) Examiner: Not Yet Assigned

**PETITION TO MAKE SPECIAL  
UNDER RULE 102(d)**

<p>CERTIFICATE OF MAILING</p> <p>I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450 ON SEPTEMBER 8, 2003.</p> <p>MARSH FISCHMANN &amp; BREYFOGLE LLP</p> <p>BY:  TERY BELICH</p>
--

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RECEIVED**

SEP 16 2003

Technology Center 2100

Dear Sir:

Applicant hereby requests that the Commissioner of Patents accord "special" status to the subject application, advancing its examination under the provisions of Rule 37 C.F.R. §1.102(d) and in accordance with Paragraph XI, Section 708.02, of the Manual of Patent Examining Procedure. A check in the amount of \$130.00 is enclosed for the fee under 37 C.F.R. 1.17(h). Please credit any overpayment or charge any underpayment to Deposit Account No. 50-1419.

In accordance with Section XI cited above, Applicant provides the following statement explaining how the invention contributes to countering terrorism.

The invention supports a system for coordinated information communications between state and federal law enforcement agencies. See Attachment A. Such information may be modified or "sanitized" depending upon who is accessing the information. In this regard, access may be denied

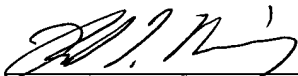
to certain information (e.g. documents), or, the information may be automatically parsed and sanitized to remove sensitive information not authorized for distribution to a particular user.

In one particular application, the invention supports a terrorist tracking system. See Attachment B. In this application, data sharing data between multiple parties, e.g., government agencies and the travel industry, is provided. Such an application allows for multiple law enforcement agencies to provide or acquire information regarding suspected terrorists. If a suspected terrorist purchases or attempts to purchase an airline ticket, appropriate information may be disseminated.

It is respectfully urged that this Petition be granted.

Respectfully submitted,

MARSH FISCHMANN & BREYFOGLE LLP

By: 

Russell T. Manning Esq.  
Registration No.  
3151 South Vaughn Way, Suite 411  
Aurora, Colorado 80014  
(720) 562-5502

Date: September 8, 2003

## **ATTACHMENT A**

## Lockheed Martin Radiant Trust® White Paper

Prepared and Submitted in support of the

### Pennsylvania and West Virginia Offices of Homeland Security Initiative

Lockheed Martin (LM) and its mission partners are pleased to submit this response to the request for a white paper describing Lockheed Martin's Radiant Trust® technology and methodology by the Homeland Security Offices of Pennsylvania and West Virginia.

#### 1.0 Introduction

This White Paper describes how the Lockheed Martin Radiant Trust® program technology and methodology would be used to securely coordinate communications and key asset protection while creating a common operational picture among local, State and Federal stakeholders to enhance situational risk assessment and management. Lockheed Martin's Radiant Trust® system combines an automated rules-based information guard function with highly sophisticated data fusion and multi-party real-time information analysis capability. The strengths of the LM solution lie in four areas: 1) unique solution, 2) powerful, flexible architecture, 3) speed of deployment, and 4) the combined experience of our team.

Radiant Trust® is an automated system capable of integrating and simultaneously analyzing databases from Government, industry, and other private sector organizations in a rules-based environment that is continuously audited for data use and information sharing policy compliance. Policies are pre-negotiated by the collaborating participants and imbedded in the Radiant Trust® application. These rules assure collaborating participants that the information they provide is shared and used only in accordance with predefined policies. Information sharing is continuously audited to assure compliance with policies governing privacy and civil liberty protection.

Lockheed Martin has designed the Radiant Trust® architecture as a strategic asset that provides a comprehensive, unique and flexible solution to satisfy the requirements of the many interrelated problem sets that comprise effective Homeland Security, e.g., terrorist detection, tracking and warning. This architecture combines leading edge technologies that allow data sharing and cross-checking for multi-modal transportation and other critical infrastructure security risk and threat assessment. For example, as applied to transportation infrastructure, Radiant Trust® applications can be quickly implemented to increase the security of the commercial travel sector and can subsequently be extended to provide enhanced security for container, pipeline, rail, trucking, shipping and other transportation modalities. The Radiant Trust® application architecture can also easily be extended to support enhanced predictive situational awareness and security of all other critical national infrastructures, such as banking-finance, communications, manufacturing, defense force protection, healthcare, etc.

LOCKHEED MARTIN PROPRIETARY

Policies and rules that govern the relationships among stakeholders, information clearinghouses and mission partners must be defined to implement a Radiant Trust® application. Lockheed Martin provides expert personnel who work directly with the application stakeholders and mission partners to help define the initial set of information sharing policies.

A uniform methodology provides consistent operational structures and environments that can be combined to exponentially increase the power and risk analysis coverage and capability of the system. The methodology considers four factors – risks, stakeholders, information clearing houses, and mission partners, as illustrated in Figure 1. Risks are typically identified in terms of risk to critical infrastructures and related assets in which stakeholders share a common interest.

# Homeland Security Initiative

Management & Data Systems

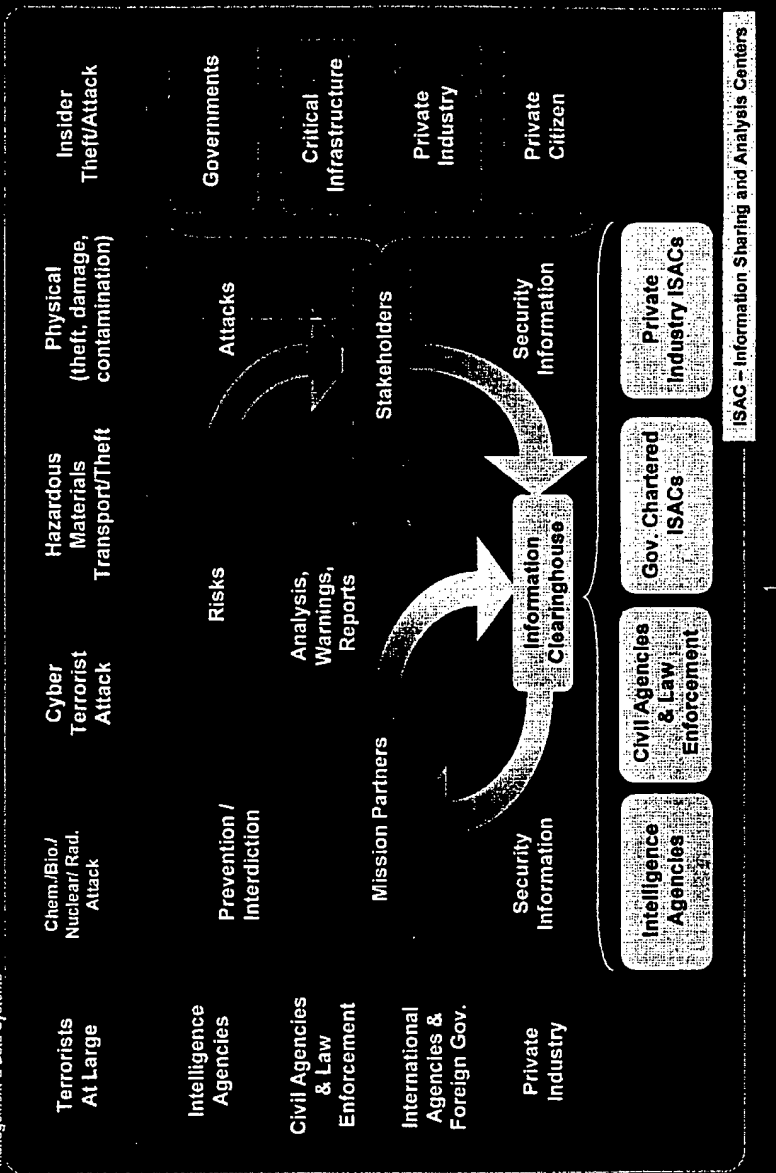


Figure 1. Risk Management Methodology

Radiant Trust<sup>®</sup>, while automating many tasks associated with developing and maintaining a common operational picture, does not replace or diminish the importance of human law enforcement and intelligence analysts. Rather, it provides a secure, trusted environment in which analysts and other mission partners can efficiently and effectively communicate, coordinate and collaborate to leverage their combined capabilities and expertise enabling stakeholders to more efficiently deploy limited resources. It also provides a powerful tool for simulating terrorist operations to exercise interdiction, crisis management and consequence management plans.

## 2.0. Radiant Trust<sup>®</sup> Technology

Lockheed Martin's Radiant Trust<sup>®</sup> provides a comprehensive, systems-engineered solution capable of supporting a wide range of integrated – and situation dependent – point solution requirements for rapid risk and threat analysis. The strategic range of Radiant Trust<sup>®</sup> supports national strategic command and control capabilities in a context capable of providing federal, state and local civil law enforcement, intelligence authorities and private sector infrastructure owner-operators with a common operational picture and threat risk assessment. As such, Radiant Trust<sup>®</sup> capabilities increase predictive threat awareness and risk management options for public and private sector Radiant Trust<sup>®</sup> participants and increase the locating, tracking and interdicting capabilities of law enforcement, national security and military organizations.

Trusted collaboration among federal, state and local government agencies and private industry organizations is promoted in the Radiant Trust<sup>®</sup> environment by embedded policies and rules governing access, sanitization, and distribution of information. Radiant Trust<sup>®</sup> is PKI (Public Key Infrastructure) enabled to authenticate and identify data originators. Radiant Trust<sup>®</sup> is ideally suited for rapid development and deployment of a national capability through locally scaled strategic applications to include Homeland security, infrastructure protection, terrorist location and interdiction. It is particularly well suited for collaboration between government agencies, industrial enterprises, and other organizations without long histories of collaboration, but who now *must* collaborate to meet today's risk assurance challenges.

Radiant Trust<sup>®</sup> provides agencies and organizations – private and public – with strategic and collaborative risk management capabilities in which the collaborative whole is more powerful and effective than the sum of the individual parts. It does this without compromising the individual agencies' or organizations' data sources or application ownership and control requirements. National agency-accredited data source control serves two very important functions: (1) It provides auditable protection of the source owner's unique and mission critical interests; (2) It provides an independently guarded and auditable mechanism for protecting the civil liberties of American citizens by assuring that data and information are accessed only in accordance with pre-defined policies, regulations, laws and procedures defined and approved by appropriate authorities. Radiant Trust<sup>®</sup> can support any strategic enterprise information management and communications coordination application that would benefit from auditable, automated data-sharing policy execution and enforcement. Radiant Trust<sup>®</sup> components<sup>1</sup> are currently supporting over 70 strategic operational installations.

---

<sup>1</sup> Radiant Mercury technology is incorporated in Radiant Trust.

The Radiant Trust® system has the flexibility to be interoperable with virtually any system. While the system has not demonstrated direct communications with airline company reservation systems, it has already demonstrated the ability to communicate with and process Passenger Name Records (PNRs) from the Galileo International Global Distribution Service (GDS) system. In this application (see Proof-of-Concept description in next section) PNR data is ingested and crosschecked against government lists to detect potential terrorists. When a suspect is detected, automatic alert messages are generated and transmitted. These alerts are tailored for the recipient and sanitized to protect civil liberties and industry proprietary data. For the proof-of-concept, alerts are generated in three different formats, for the demonstration recipients – XML, e-mail, and pager/cell phone text messages.

Radiant Trust® was designed with data quality validation as an integral function. In addition, the system was designed with an integral capability to be interoperable with disparate data sources and data formats. The Radiant Trust® system was designed for and is scaleable to handle real-time transaction processing, and is used in real-time applications for several government agencies.

The Radiant Trust® technology was developed to protect the Nation's most sensitive data while promoting the sharing of allowed information. This technology was developed in close coordination with several government agencies involved in information security/information assurance. This technology has been extensively tested and proven to provide the highest levels of data protection and security. The rules-based technology is used to define and enforce the required policy, whether it concerns civil liberties, national security, legal restrictions or industry proprietary information. The system complies with the TCSEC requirements for security, protection against unauthorized access or disclosure of information, at the B-1 level. In addition to these capabilities, the system also has an extensive audit capability that can be used to demonstrate continued proper policy implementation.

Radiant Trust® provides the ability to connect to multi-protocol (and multi-level) LANs and WANs. The Radiant Trust® message sanitation and distribution guard technology is Radiant Mercury, the only system that has been formally evaluated and profiled by NSA to automatically downgrade information from one security level to another. It guarantees the separation and protection of the data from the moment information enters Radiant Trust® until it is released to the output system using both application-specific and trusted Operating System-specific features. Within Radiant Trust® the data transformations and releases are controlled by rules that implement and enforce government and industry specified data protection and sanitization policies. The system has been extensively tested by NSA to ensure that unauthorized access is prohibited. Changes to the rules are under two-person control and all actions are audited. Unrecognized data formats are not permitted to enter the system.

Policies are defined by the data source owners, and those policies are translated into rules within Radiant Trust® that become the basis for processing or passage of any data through the Radiant Trust® system. These adaptable rules and policies are executed and continuously audited by the system. The result is a trusted, real-time information sharing and analysis capability with an explicit audit function that accommodates the source data ownership and control needs of



participating agencies while providing National Agency accredited multi-level security data distribution capability and explicit safeguards for citizen privacy and civil liberties.

### 3.0 Proof of Concept

Lockheed Martin and its partners currently have an ongoing proof-of-concept demonstration of the Radiant Trust® program focused on reducing the risk of terrorist attacks against airlines. We recommend that this capability be included in the Pennsylvania and West Virginia Homeland Security pilot project. This application will provide valuable learning and experience to the Pennsylvania and West Virginia Homeland Security Offices, and participating State, local and Federal agencies. It will also immediately enhance Federal and State law enforcement agencies' ability to locate, track and interdict terrorists and suspected associates who attempt to use the global commercial transportation reservation systems to plan air, rental car, hotel, tour and related transportation logistics.

While this program will significantly improve commercial air travel safety, it also serves as a working model of public-private sector cooperation to more effectively assess and manage risk and threats to all transportation infrastructures, modalities and associated economic, physical and cultural targets. This program brings together key technologies and partnerships to provide a powerful, scalable transportation risk assessment and management solution.

Since January 2002, Lockheed Martin and its partners have operated a pilot demonstration located at Galileo International, one of the leaders in the travel reservation system industry. This proof-of-concept pilot is a collaborative effort between Lockheed Martin, Galileo International and Systems Research & Development (SRD) to demonstrate the capability to securely crosscheck passenger reservation information against sensitive government information (such as known or suspected terrorists and their suspected associates) in real time. Automatic, tailored notifications are generated for the appropriate government agencies when matches are detected. Radiant Trust® technology provides the required automated data-sharing ability while simultaneously protecting sensitive data of all parties. At no time is sensitive government information apparent or accessible to any party other than authorized government agencies. All crosschecking and analysis is performed on isolated computers in compliance with duly authorized government policy. Similarly, sensitive industry information is protected from release by the same technology that has been certified and accredited by the U.S. Government.

The architecture of this proof-of-concept pilot was designed to be extremely flexible. Additional data sources (e.g., direct inputs from freight forwarders, bank payment/settlement companies, rail and rolling stock companies and airline companies) can be easily added. New message formats or data structures can be added to the Radiant Trust® system using a table-driven parser, without requiring software modifications. In the proof of concept application built by Galileo International, SRD and Lockheed, SRD's NORA™ technology is used to cross check industry reservation data and government suspect identification data and to evaluate relationships in the data that may not be immediately obvious to human analysts. In a production application the SRD software can be augmented or replaced with other name matching, and analysis software as required by the mission requirements of the production application.

Radiant Trust® makes adding additional data sources and analysis software, such as the University of Pittsburgh data on key assets and mapping software, straight forward. New data structures can also be added to the system easily. In addition, Radiant Trust® can automatically "transliterate," or change the format, of messages as they pass through the system to allow connectivity among systems that otherwise would be incompatible with each other, eliminating the need to modify existing industry or government software.

A major strength of the Radiant Trust® technology and methodology is that it enables threats from multiple domains to be simultaneously evaluated and addressed. For example, Lockheed Martin and the Computer Emergency Response Team (CERT) at Carnegie Mellon University are working on applying Radiant Trust® technology to enhance CERT's already world-class cyber threat detection and warning capability. We strongly recommend that this work be sustained and integrated into the Pennsylvania-West Virginia Homeland Security program. As Homeland Security executives from both States and the Federal Government are aware, the likelihood of combined physical and cyber attack is very strong, and the CMU CERT is ideally situated to provide world-class safeguards against such threats while simultaneously safeguarding the Radiant Trust® systems themselves from cyber attack.

#### **4.0 Centers of Excellence**

Lockheed Martin has established a Radiant Trust® Center of Excellence (RTCE®) at the West Virginia University Lane Department of Computer Science and Electrical Engineering and the College of Business and Economics. This Center of Excellence is focused on developing continuous auditing capabilities focused on business workflow processes to include supply chain processes, financial processes, and other business workflow processes. As such the WVU Radiant Trust® Center of Excellence is ideally suited for developing continuous auditing capabilities specifically tailored to meet the needs of the private sector participants in the Pennsylvania-West Virginia Homeland Security Project.

Lockheed Martin and CMU/SEI/CERT are establishing a Carnegie Mellon Radiant Trust® Center of Excellence. This Center of Excellence will be focused on establishing information and information systems security best practices that can be implemented as continuously audited rule sets in Radiant Trust® Homeland Security applications. The CMU and WVU Radiant Trust® Centers of excellence are, therefore, ideally situated to provide world class policy definition and implementation to the Pennsylvania-West Virginia Homeland Security Project and to other State and federal programs as they are implemented based on the success of the Pennsylvania-West Virginia leadership initiative.

Lockheed Martin is also establishing a Radiant Trust® Center of Excellence with the University of Pennsylvania, Wharton School, Wharton Risk Management and Decision Processes Center and the Columbia University Center for Hazards and Risk Research. This Center will be focused on developing risk management analysis and valuation models and capabilities that will facilitate better understanding of the extreme risks posed by modern threats to critical infrastructures, extended commercial and economic supply chains, etc., as well as the relationships between various types of risks and efficient insurance, reinsurance and other mitigation strategy pricing.

The individual and combined capabilities of these Radiant Trust® Centers of Excellence, all located in Pennsylvania and West Virginia, significantly enhance the probability of success for the Pennsylvania-West Virginia Homeland Security project. They also provide a lasting basis for long-term leadership and value to other states and nations wishing to establish effective Homeland Security programs based on the model established by Pennsylvania and West Virginia. We strongly recommend that Pennsylvania and West Virginia support the activities of these Centers of Excellence as part of this initiative.

### **5.0 Standards Development**

Lockheed Martin believes that standards of best practice must be developed and enforced to assure consistent predictive and forensic capabilities of systems supporting Homeland Security. For this reason Lockheed Martin endorses and supports the leadership of Pennsylvania and West Virginia in establishing and supporting the National Cyber Forensics Training Alliance and the world class information assurance research and capabilities developed at Carnegie Mellon University (CMU) and West Virginia University. We believe that these Nation leading cyber security initiatives will play an important role in the Pennsylvania-West Virginia Homeland Security project contemplated by this whitepaper. We draw special attention to the world-class work being done at the Computer Emergency Response Team (CERT) at CMU's Software Engineering Institute. We believe that CERT participation is essential to this initiative.

- Carnegie Mellon University/Software Engineering Institute/CERT – A Radiant Trust® Center of Excellence (RTCE) that will focus on developing standards of best practice for information and information systems security and hardening the cyber infrastructures that underpin critical infrastructure operations, control and predictive analysis and warning applications of Radiant Trust® for law enforcement, intelligence and the private sector.

### **6.0 Privacy and Civil Liberties Policy Development**

No issue is as important - or as potentially challenging - to effective and lasting Homeland Security programs as the protection of individual privacy, commercial confidentiality and citizen civil liberties while increasing the security of public and private infrastructures and assets. To paraphrase one of Pennsylvania's most famous sons, a principle founding father of our Nation, sacrificing the liberties that define our way of life and our future potential for additional security is a poor bargain. Radiant Trust® is particularly well suited for Homeland Security applications. As a policy driven system, it enforces policies defined by the participants. These policies are designed and reviewed by competent authority to safeguard the privacy and civil liberties of the populations being protected. Radiant Trust® enforces oversight policies of trusted third parties whose role is to assure that civil liberties are not abused. Adding an oversight policy layer is strongly recommended. All policies imbedded as rules in Radiant Trust® are continuously audited to assure compliance.

Much of the work associated with implementing a Radiant Trust® application will be focused on developing the operational and oversight policies and rule sets. It is strongly recommended that this initial application be kept as simple and straightforward as possible to permit Pennsylvania and West Virginia personnel the opportunity to gain necessary practical experience in this important process. We are very encouraged by the professional experience and commitment of

the Pennsylvania and West Virginia Homeland security personnel we have met and are confident that these personnel are extremely well qualified for this important aspect of the project.

It is also important to note that two Radiant Trust® Centers of Excellence – one at West Virginia University and one at Carnegie Mellon University are specifically focused on developing lexicons and policy guidelines for this type of public-private sector collaborative application. These Centers of Excellence will be significant resources for Pennsylvania and West Virginia as this project is implemented and for the Nation as other State programs and a National program are implemented.

- West Virginia University – An RTCE® focusing on research on hardened continuous and real-time business process auditing for applications of Radiant Trust® aimed at manufacturing supply chains, secure medical and pharmaceutical research application, Homeland Security Policies and economic and financial risk management concepts and practices.
- Wharton-Columbia Graduate Schools of Business – An RTCE® that will focus on extreme risk management practices and valuation models and methodologies to support insurance, reinsurance and other risk management strategies, programs and policies.

## **ATTACHMENT B**

Original (Draft)

11 March 2002

# **PROPOSAL**

for the

## **RADIANT TRUST IMPLEMENTATION**

of a

## **TERRORIST TRACKING CAPABILITY (TTC) PILOT**

## TERRORIST TRACKING CAPABILITY PILOT

### 1 Terrorist Tracking Capability Pilot

This unsolicited proposal describes the functionality and benefits afforded by the creation of the Terrorist Tracking Capability (TTC) Pilot. The TTC Pilot provides a trusted accreditable, direct, secure method of sharing data between industry and government, while simultaneously protecting the sensitive information of all participants. This data sharing identifies potential terrorist travel activities and provide notifications of those activities in real time.

### 2 Submitting Agency and Points of Contact

Lockheed Martin Space Systems Company, P.O. Box 179 Denver, CO, 80201-0179

Name	Function	e-mail	Phone number
Kevin Flesher	Marketing Lead	<a href="mailto:kevin.e.flesher@lmco.com">kevin.e.flesher@lmco.com</a>	(303) 977-0916
William D. Scott	Program Manager	<a href="mailto:william.d.scott@lmco.com">william.d.scott@lmco.com</a>	(303) 977-0623
Chip Auten	Chief System Engineer	<a href="mailto:chip.w.auten@lmco.com">chip.w.auten@lmco.com</a>	(303) 971-2858

### 3 Sponsoring Organization/Agency and Points of Contact

Office of Homeland Security

### 4 Identification of Proprietary Data

This proposal contains Lockheed Martin (LM) Proprietary Data. LM Proprietary data is:

- Proposed Price and all supporting pricing data such as rate information, effort Basis of Estimates (BOEs)
- All information regarding the proposed design generated by LM.

### 5 Identification of Agencies Receiving Proposal

Additional agencies or parties that may receive this proposal:

- Federal Bureau of Investigation (FBI)
- Department of Justice (DOJ)
- Department of Defense (DoD)
- Global Distribution Systems (GDS) – commercial reservation service providers:
  - Galileo International
    - A subsidiary of Cendant Corporation
    - Headquartered in Parsippany, New Jersey, USA

- Worldspan
  - Headquartered in Atlanta, Georgia, USA
- Sabre
  - Headquartered in Dallas/Ft Worth, Texas, USA
- Amadeus
  - Regional Offices in Miami, Florida, USA
  - Headquartered in Madrid, Spain

## 6 Authorization

Signature, title of person signing and date

## 7 Technical

### 7.1 Abstract

Lockheed Martin (LM) proposes to create a Terrorist Tracking Capability (TTC) that provides automatic notification of potential terrorist travel activities. This proposal describes how the Lockheed Martin Radiant Trust<sup>®</sup> program technology and methodology would be used to securely coordinate communications and key asset protection while creating a common operational picture among local, State and Federal stakeholders to enhance situational risk assessment and management. Lockheed Martin's Radiant Trust<sup>®</sup> system combines an automated rules-based information guard function with highly sophisticated data fusion and multi-party real-time information analysis capability. The strengths of the LM solution lie in four areas: 1) unique solution, 2) powerful, flexible architecture, 3) speed of deployment, and 4) the combined experience of our team.

The TTC provides the mechanism to allow (and control) sharing of data between the travel industry and government agencies responsible for interdiction of terrorists. The TTC uses mature trusted technology to assure the protection and security of critical public and private infrastructures, and intellectual property while protecting the civil liberties of the traveling public.

The TTC provides a secure network between the four GDS', that account for 95 percent of worldwide air travel reservations, and the FBI, CIA and TSA. The secure network provides real-time notification of potential terrorist's travel reservations to these government agencies. These notifications allow the agencies to interdict the terrorist before they board an aircraft, or to track their movements if interdiction is not appropriate. The system detects multiple terrorist reservations on a single flight, thereby identifying additional potential risk to that flight.

LM proposes to adapt existing technology, integrate and deploy the components of the TTC and maintain those components for the remainder of FY 2002.



Lockheed Martin has designed the Radiant Trust® architecture as a strategic asset that provides a comprehensive, unique and flexible solution to satisfy the requirements of the many interrelated problem sets that comprise effective Homeland Security, e.g., terrorist detection, tracking and warning. This architecture combines leading edge technologies that allow data sharing and cross-checking for multi-modal transportation and other critical infrastructure security risk and threat assessment.

## **7.2 Objectives**

The objective of the TTC is to reduce the risk associated with terrorist activities such as those that occurred on 11 September 2001. The ability of the TTC to identify terrorists and support the interdiction of those terrorists reduces the physical risk to the public, the economic risk to the travel industry and the economic risk to the U.S. TTC provides the technology to leverage currently available information in the identification of potential terrorist travel activities and to automatically notify the appropriate agencies of those activities in real time and in advance of the event.

The objective of the TTC Pilot is to allow the TTC participants to evaluate the technology and determine if the technology should be retained and expanded to cover all U.S. critical infrastructures.

## **7.3 Approach**

LM proposes to use technology developed for the Radiant Mercury System as the basis for the Radiant Trust® component of the TTC Network. Radiant Trust® provides the capability to automatically sanitize sensitive data, transliterate message formats, create appropriate alert notification messages and guard all outgoing messages for inappropriate information.

This technology has been evaluated by the National Security Agency (NSA), and accredited for automatic sanitization of Sensitive Compartmented Information (SCI) data by NSA, NRO, DIA, CIA and NIMA.

Radiant Mercury is the only system of its type on the Office of the Secretary of Defense (OSD) migration list. This mature technology has been in use for nine years at sites around the world.

In addition to the Radiant Trust® System, LM proposed to integrate a second component that performs cross-checking of passenger information with government watch lists. When potential matches are detected, an alert notification is generated and transmitted to the appropriate TTC participants. Initially, it is expected that the recipients are the FBI, CIA and TSA.

The system has been designed to handle all tailored notifications that may be sent to additional agencies and locations, as policy evolves in the future. These may include local offices of the FBI, state and/or municipal law enforcement agencies, and airport passenger security screeners.

## 7.4 Expected Results

Notifications generated by the TTC can be used to interdict terrorists. This reduces the risk of terrorists being able to move freely and unobtrusively throughout the world. The TTC provides anti-terrorist agencies with the capability to detect and monitor terrorist movements around the world. Participation by all four GDS' provides 95% coverage of all airline reservations worldwide.

A key feature of the proposed TTC is the ability of the Radiant Trust® component to audit policy enforcement and all message traffic passing through the system. This audit capability provides specific data that can be used to demonstrate that the TTC has statistically lowered the risk to the air travel industry. The ability to provide this data can then be used by the insurance industry to justify lowering the risk rating of the air travel industry. This should result in lower post-9/11 insurance rates, critical for the economic survival of the industry.

No issue is as important - or as potentially challenging - to effective and lasting Homeland Security programs as the protection of individual privacy, commercial confidentiality and citizen civil liberties while increasing the security of public and private infrastructures and assets. Radiant Trust® is particularly well suited for Homeland Security applications. As a policy driven system, it enforces policies defined by the participants. These policies are designed and reviewed by competent authority to safeguard the privacy and civil liberties of the populations being protected. Radiant Trust® enforces oversight policies of trusted third parties whose role is to assure that civil liberties are not abused. Adding an oversight policy layer is strongly recommended. All policies imbedded as rules in Radiant Trust® are continuously audited to assure compliance.

Much of the work associated with implementing a Radiant Trust® application will be focused on developing the operational and oversight policies and rule sets.

It is also important to note that two Radiant Trust® Centers of Excellence - one at West Virginia University and one at Carnegie Mellon University are specifically focused on developing lexicons and policy guidelines for this type of public-private sector collaborative application.

In addition to the insurance aspect, the audit data can be used to justify additional security checks for suspected passengers. If the additional checks are questioned, the audit data can be used to show that there was specific and credible justification for the action.

## 8 TCC Key Personnel

The following key personnel are proposed to be involved with the TCC Pilot:

Function	Name	Experience	Key Skills/Qualifications/Education
Program Manager	William (Bill) D. Scott	25 years	Hardware Design Lead/ Manager Performance Modeling Group BS Logistics Management

Deputy Program Manager/ Chief System Engineer	Charles (Chip) W. Auten III	22 years	System Engineering, Process, Installation & Training/ 9+ years with Radiant Mercury (RM) Program/ BS Aerospace Engineering MS Technical Management
Chief Architect			
Software Lead	Thomas (Tom) A. Marso	22 years	Trusted Multi-Level Secure Software Development, Installation/ 8+ years on RM Program, including the original RM development team/ BS
Installation Coordinator			
Training Lead			
Lab Manager/Hardware Acquisition	Greg R. McBroome	?? years	

## 9 Government Support

In order to create the TTC Pilot, the following is required from the Government:

- Provide to LM a definition of the Policies that the Radiant Trust® System implements and enforces.
- Identify to LM the message formats used for watchlists in an Interface Definition Specification (IDS) document.
- Provide watchlist data in an electronic form to the TTC.
- Provide alert formats and data contents in an IDS document.
- Identification to LM of any requirements not listed in the Operational Requirements Document.

## 10 Industry Support

Industry is responsible for providing appropriate space for the Radiant Trust® and related components at the GDS that meets the requirements defined in the Physical Requirements for the Terrorist Tracking Capability (TTC) Industry Participant Nodes (IPN) Specification and the Passenger Name Record (PNR) format for the electronic transmission of PNRs to the TTC Pilot.

## 11 Supporting Information

The following supporting documentation is available:

- System Design Description
- Operational Requirements Document
- Statement of Work for the Radiant Trust® Implementation of a Terrorist Tracking Capability Pilot
- Schedule
- Price Basis of Estimate

#### **11.1 Estimated Cost**

Price and period that proposed price is valid

The basis of estimate for this price is available upon request.

#### **11.2 Preferred Contract Type**

Fixed Fee Cost Plus (FFCP)

#### **11.3 Proposed Period of Performance**

LM proposes to complete the creation of the TTC 150 days from date of delivery of GFI.

#### **11.4 TCC Team Organization**

The Radiant Trust® Organization is depicted in the following diagram. Key personnel have been selected for their expertise and experience. The Software Lead has extensive experience on the Radiant Mercury program, from which the Radiant Trust technology is derived. The Chief System Engineer also came from the Radiant Mercury program.